Centers for Medicare & Medicaid Services
Office of Information Services
Consumer Information & Insurance Systems Group
7500 Security Blvd
Baltimore, MD 21244-1850

State Testing Handbook

Version: 1.0
Last Modified: February 26, 2013

APPROVALS

Submitting Organization's Approving Authority:

Signature	Printed Name	Date	Phone Number

<Position Title> *[e.g., <CMS Business Owner>]*

REVISION HISTORY

Version	Date	Organization/Point of Contact	Description of Changes
1.0	2/26/2013	CMS OIS State Engagement Team	Final version published

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The Affordable Care Act creates new competitive private health insurance markets, known as Exchanges, which will provide millions of Americans and small businesses access to affordable coverage and the same insurance choices that members of Congress have. Exchanges will help individuals and small employers shop for, select, and enroll in high quality, affordable private health plans that accommodate their needs at competitive prices.

Individual States must meet Federal standards and statutory requirements as they apply to the different Exchange models.

State systems, supporting the State Based Exchanges (SBE), Medicaid and Children's Health Insurance (CHIP) programs, other State agencies, and Issuer systems (collectively referred to as stakeholder systems) will interact with the Federal Data Services Hub (FDSH), which provides common services and interfaces to Federal agency information (Trusted Data Sources or TDS). Stakeholder systems will utilize business services offered by the FDSH to request information from various TDS for determination of exemption, eligibility, and enrollment; and to exchange electronic accounts, where applicable. Some stakeholder systems will also send information to the FDSH for financial management, reporting and payment.

For those States who elect not to provide an Exchange for individuals residing in that State, the Federal government will provide a Federally Facilitated Exchange (FFE). The Federal Exchange Program System (FEPS) consists of an FFE--serving the needs of citizens within States which do not have their own State-run Exchange--and the FDSH.

FEPS operates to support the provisions of the Affordable Care Act and does not replace any existing or current systems within the Centers for Medicare & Medicaid Services (CMS).

1.1 OVERVIEW AND SCOPE

The State Testing Handbook is part of a Testing Package which has been designed to assist States during the FEPS testing lifecycle and includes prescriptive how-to steps, checklists, operating procedures, guidance and references. The State Testing Handbook is one of several artifacts utilized within the FEPS testing lifecycle. Others artifacts, including more general reference material, that are applicable to all States include the "*State Testing Process and Test Data*" (test data summary) document, "*CMS Onboarding Guide to the Hub*" and a series of "*CMS Exchange User Guides and Reference Manuals*" that are in draft development as of version 1.0 of this Handbook.

Artifacts that are developed uniquely for each State include the State Testing Profile, FEPS-and-Partner Test Plan and Schedule and the Test Readiness Review documents for Secure Communication and FEPS-and-Partner Testing. This set of material produced for each State is provided during the introduction and orientation portion of a State's test execution period. A sample State Testing Profile and Test Readiness Review form are included within this Handbook, within appendices D & E respectively.

It is important to understand that FEPS testing covers a specific segment of testing that States are responsible for performing involving the federally provided systems in the FEPS environment, the FFE and the FDSH. It is different from the testing that a State conducts associated with local systems development projects and, although related, it is not the equivalent of Business Operations testing, such as Blueprint Test Scenarios, which correspond to functional tests to demonstrate that responsible State entities can conduct their respective areas of business in a production environment. The State Testing Handbook covers testing planned around the structural and logical interfaces and workflows between each State and FEPS. It includes a comprehensive view of the CMS-manufactured test data set that links a common set of test data with FEPS test cases and scenarios[1] based upon a State's interactions identified in the State Testing Profile. The results that are documented in the FEPS Test Summary Report for FEPS testing will provide a standalone assessment of technical capability progress which will also be utilized and incorporated into appropriate portions of more broadly scoped Business Operations testing, such as Blueprint Test Scenarios, as well as Preliminary and Final Operations Readiness Reviews.

The scope of the State Testing Handbook includes guidance, direction and information collection, that at a minimum covers:

- High-level State Testing Profile details such as Exchange types and related system interactions
- Data exchange patterns that isolate the available communication and transfer models
- FEPS test scenarios, scripts, cases, and data by interactions for use in system testing
- Testing infrastructure connectivity including required security measures
- Checklist of items in detail that builds different Test Readiness Review artifacts
- Defect tracking and management
- Testing timelines with key dates

1.2 AUDIENCE

The State Testing Handbook is relevant to all States participating in formal testing with FEPS and includes the States that are planning to utilize the FFE, including State Partnership Exchanges (SPEs), States building SBEs, Issuers, and Medicaid and CHIP agencies.

[1] Unless specifically noted as Blueprint Test Scenarios and Test Cases, scenarios and cases refers to FEPS Test Scenarios and Test Cases

2 STATE TESTING OVERVIEW

States have significant flexibility in the development of Exchanges to meet the needs of their citizens. The Department of Health and Human Services (HHS) has developed a program that offers multiple Exchange models as well as a number of design alternatives within each of those models. Exchanges will operate either through a SBE or a FFE. A State may also operate in partnership with the FFE as a SPE, which provides States with the option to administer and operate Exchange activities associated with plan management activities, some consumer assistance activities, or both. HHS, as the party responsible for Exchange implementation, will provide as much flexibility as possible; however, HHS will need to ratify inherently Federal governmental decisions made by the SBE State.

Regardless of the model selected by the State, formal testing must occur to ensure:

- Connectivity
- Correct data exchange formats and values
- Correct interpretation of responses from the FDSH
- Correct interpretation of any error messages from the FDSH
- Correct information is provided in regard to defect management and re-testing requirements

2.1 ROLES AND RESPONSIBILITIES

Well-defined roles with corresponding responsibilities and known, understandable and measurable communication paths are required to ensure that States are provided the opportunity for a successful FEPS testing experience. Table 1 below lists individuals assigned as Team Leads for the different components of the FEPS testing lifecycle.

Table 1 - Roles and Responsible FEPS Team Leads

Role	Responsible FEPS Team Lead
State Engagement Testing Manager	CIISG – Kirk Grothe Phone: (301) 492-4377 Email: kirk.grothe@cms.hhs.gov

Testing Coordinators	CIISG – Paul Donohoe Phone: (410) 786-6344 Email: Paul.Donohoe@cms.hhs.gov CCIIO – Jenny Chen Phone: (415) 744-3689 Email: Jenny.Chen@cms.hhs.gov CCIIO – Andrea Greene-Horace Phone: (301) 492-4112 Email: Andrea.Greene-Horace@cms.hhs.gov CMCS – Jessica Kahn Phone: (410) 786-9361 Email: Jessica.Kahn@cms.hhs.gov
Technical Integration	CIISG – Paul Donohoe
Testing Execution	CIISG – Mark Oh Phone: (301) 492-4378 Email: mark.oh@cms.hhs.gov
Test Monitoring	CIISG – Kirk Grothe
Development Team Technical Manager	CIISG – Mark Oh
Testing Executive	CIISG – Monique Outerbridge Phone: (301) 492-4376 Email: monique.outerbridge@cms.hhs.gov

2.2 CALT AND CMS SERVICE REPOSITORY

CMS's Collaborative Application Lifecycle Management Tool (CALT) manages the dynamic environment of on-going project and application development related to the many areas of health care managed by CMS. The tool is used to track and manage the lifecycle of new applications as well as the changes and upgrades made to existing software applications.

FEPS project collateral is stored in the CALT repository under the "Exchange Community" (https://calt.cms.gov/sf/go/proj1013) and "Medicaid State Collaborative Community" (https://calt.cms.gov/sf/projects/medicaid_state_collaborative_com) Projects. Once granted access to CALT, the State user must be granted access to the "Exchange Community" and/or "Medicaid Community" projects in CALT.

CALT may be accessed at: https://calt.cms.gov/sf/sfmain/do/home

CALT contact information is as follows:
Email: Calt_Support@cms.hhs.gov
or
XOSC Helpdesk
Phone: 1-855-CMS-1515 (1-855-267-1515)

The CMS Service Repository is the primary tool for state/vendor IT developers to access:

- Business Service Definitions
- SOAP UI Test Scenarios
- Service Endpoint configurations
- WSDL Service Description Files
- XML schema files

To obtain access, request user ID:

1. Complete the Service Catalog User application form located here: https://calt.cms.gov/sf/go/doc15784?nav=1
2. Send completed application to the following email address: dshsupport@qssinc.com . States should copy their OIS IT PM and Medicaid E&E Systems Analyst when making the request.

*Access is limited to state users and their contractors

2.3 TYPES OF TESTING

The complete scope of FEPS testing includes several required test types (secure communication, FEPS-and-Partner integration and Production Readiness) and others where State involvement will be dependent upon readiness criteria. In whole there are four (4) test types involving States that will be conducted leading up to Open Enrollment:

- **Secure Communication.** Secure Communication Testing verifies whether both sides (CMS and State) have the communication ports/protocols open for subsequent Test Types in the State and CMS Formal Testing environments. If a State testing environment changes it will require a subsequent Secure Communication test.

  In most cases, Secure Communication Testing will involve three variations of Testing:

  - **Type 1:** Basic ‘Ping’ Test at the Port layer.
  - **Type 2:** Certificate/Key Exchange Test at the Transport (or Network) layer.
  - **Type 3:** Certificate/Key Exchange Test at the Services (or Application) layer.

  In other cases, Secure File Transfer Protocol (SFTP) Testing will be conducted, i.e. for States simply exchanging files to/from the FDSH.

  States will have the option to test Certificates/Key Exchanges during the FEPS-and-Partner phase of testing, if not fully prepared to do so during the Secure Communication phase.

- **FEPS-and-Partner.** FEPS-and-Partner Testing is designed to test a State's system functionality and State's business logic interoperability. Scenario-driven test cases will be used to verify both software and hardware interoperability. In most cases, CMS will coordinate the Test Data sets, Test Cases, and Test Scenarios. FEPS-and-Partner testing may, if appropriate for the State, also be merged with Business driven Scenarios and Test Cases, such as with the Blueprint Test Scenarios. FEPS-and-Partner Testing for services is further broken down into the following sub-categories:

  - FEPS-and-Partner Core Verification and Eligibility Interactions
  - State-Specific Interactions for Medicaid/CHIP Agencies in FFE States State-Specific Interactions for SBE
  - Issuer-Specific Interactions

  It will be the responsibility of each State to deploy the Test Data into their respective User Interface (UI)/applications and/or back-end systems.

  FEPS-and-Partner FDSH Services includes:

  - Verification of the interoperability of the State's system functionality, hardware and software, and business logic with the FDSH
  - The State's usage of their UI/application or back-end systems and CMS provided test data to produce the payload[2] required to invoke FDSH services and subsequently consume the response from the FDSH service

    Please note that a standalone tool or utility is not appropriate for Formal testing and State's working with this type of interoperability testing should use the Informal environment.

- **End-to-End**
  End-to-End Testing verifies system functionality and interoperability across a Multi-Partner environment, i.e. with all Partners. Testing will be based upon Eligibility and Enrollment scenarios to ensure that:
  - The Federally Facilitated Exchange (FFE) (optionally State Based Exchanges (SBEs), M&C) can consume a full range of applications and generate appropriate requests to FDSH ;
  - The FDSH can generate requests to States;
  - States can generate responses from their test data bases and the FFE can generate correct outcomes.

  Approximately 330 – 1,000 test data applications[3] with identical functional data will be provided to each eligibility source (FFE/SPE, SBE and M&C). The test data applications

[2] the actual data that is encapsulated in a packet and transmitted on a network

[3] truncated application format that will be sufficient for States to invoke the FDSH services

will cover paths that match the data embedded in the Partners test environments and include additional individuals and Tax Households that will not match.

Examples of paths that match and do not match data embedded in the Partners test environments:

- Positive match for a service: John Doe is verified as a citizen by Social Security Administration (SSA).
- Negative match for a service: John Doe's name and birth-date do not match. Verification is unable to be made by SSA. Error code is generated.
- Positive match for an application: All verifications by Federal Partners and States are able to be invoked for John Doe. John Doe is deemed eligible for QHP by the Exchange and receives APTC.
- Negative match for an application: John Doe is required to go to DHS' Step 3 service for verification of lawful presence. The Step 3 service is unable to deem his lawful presence. A 90 day inconsistency period is triggered and eventually the application is timed out due to inaction on John Doe's part.

The planned End-to-End test start date is August, 2013. At the beginning of End-to-End testing, Regression testing will be conducted in a one-to-one (CMS/State) manner. Regression testing at this point in the test cycle will provide an opportunity for States to re-test services that have gone through refactoring since they were initially tested.

- **Production Readiness**
  Production Readiness Testing verifies connectivity between the Federal Exchange Program System (FEPS) production environment and other Partners' production environments. The planned Production Readiness test start date is September, 2013

Note: The current version of the Testing Handbook, 1.0, covers details relevant to Secure Communication and FEPS-and-Partner. Additional information pertaining to End-to-End and Production Readiness is forthcoming and will be provided in addendums to the State Testing Handbook.

2.4 FEPS TESTING EXPECTATIONS

Ongoing coordination is essential for State testing to be successful. Resources from multiple organizations within each State will be responsible for:

- Assisting with the finalization of the FEPS-and-Partner Test Plan and Schedule as well as ensuring that activities, tasks and milestones within the Schedule that are owned by the State are completed in a timely manner
- Meeting pre-requisite readiness requirements
- Repairing defects in their respective systems
- Keeping test systems operational, and
- Providing necessary levels of database and/or UI/application administration. Appropriate stakeholders within each State will provide resources to manage and maintain their

respective Interface Control Documents (ICDs) and Business Service Descriptions (BSDs). CMS and State's collaboration will be required to define the threads that connect test scenarios, test scripts, test cases, and test data from the pre-determined inventory that match appropriate interaction points between CMS and the State.

3 TEST ONBOARDING

3.1 TEST ENVIRONMENT

Each State agency will provide a Testing Environment. The State agencies will use their own environments, and information about the locations and their access requirements will be coordinated with CMS prior to engaging in State testing. The State agencies' test environments will contain all Exchange related applications, interfaces, and data necessary for the execution of the scheduled test type.

CMS will use the Implementation test environment, which contains all FEPS applications, interfaces, and data. This environment is designed to mirror the live production environment, including interfaces with Federal agencies (for applicable Test Types) and external business partners as well as controls on data flow and volume. This environment will support testing of:

- Internal FEPS interfaces and data flows
- External interfaces and data flows
- New releases and production fixes
- Performance Stress testing volume loads

Pertinent connection information about the CMS Implementation environment will be transmitted to the States within the FEPS-and-Partner Test Plan document.

3.2 TESTING ENVIRONMENT OPERATIONS AND CONFIGURATION CHECKLIST

There are numerous test environment details that require documentation prior to engaging in test execution. These "operation and configuration" details are applicable to each type of testing and will vary depending upon the data exchange pattern that is being invoked for certain interactions. It is also possible that there will be different State systems involved in the various interactions which may require collecting multiple sets of data.

All of the test types described in section 2.3 have a FEPS and State endpoint. Therefore the operations and configuration information is required for all environments planned to be involved in the testing. The operations and configuration information pertinent to each State will be acquired through the State Testing Profile (see Section 4) and merged into a Master Profile database managed by Regional Technical Support (RTS). The State's OIS IT PMs or Medicaid E&E Systems Analysts with support from RTS will interface with States one-on-one to review and document all essential Operations and Configuration details based upon their specific characteristics within the States Testing Profile.

The FEPS Testing environment operations and configuration detail will be documented within the FEPS-and-Partner Test Plan.

3.3 SECURITY CHECKLIST

- Security standards that are required to perform testing of the FDSH Secure Web services include the following:
  - ➢ WS Security 1.1
  - ➢ Password Hashing Algorithm: Base64 encoded, SHA-1
  - ➢ WS Security UserNameToken Profile 1.1
- State testers should use the same current working directory for all command prompt items
- The State should generate a local self-signed certificate for testing; although, a third-party certificate will be required for End-to-End testing and entering the Production environment.

4 STATE TESTING PROFILES

The State Testing Profile will capture all information required to prepare and plan for testing engagement with an individual State and will include information that covers each of the test types that the State is scheduled to participate in. The information in the Profile will be collected in a standardized manner several weeks prior to beginning actual test execution and will form the basis for unique customization and tailoring of an individual State's FEPS-and-Partner Test Plan.

The majority of data collection presented in the Profile will be associated with;

- Technical integration detail
- Drill-down of related selections initially characterized by Exchange types with subsequent choices that outline interactions, data exchange patterns, scenarios/scripts/cases/data and other test execution characteristics

For a sample copy of the State Testing Profile Template refer to **Appendix E – State Testing Profile Template.**

The remaining sub-sections provide additional details about the FEPS interactions that will appear within the State Testing Profile document for different Exchange models.

4.1 FEPS-AND-PARTNER CORE VERIFICATION AND ELIGIBILITY INTERACTIONS

The table of FEPS to Federal Partner Core Verification and Eligibility Interactions provides a list of all of the interactions with the FDSH that are common across SBE, FFE & SPE States and Medicaid/CHIP (M&C) Agencies. This list allows the reader/tester to understand the scope of interactions. These interactions may be real-time services or batch-processed data exchanges. The data exchange model applicable to each interaction is provided in the State Testing Profile at the time they are distributed to each State.

Note: All services listed were confirmed as of 02/22/2013. For the most recent list of services search for “service forecast” on CALT (https://calt.cms.gov)

Table 2 – FEPS-and-Partner Core Verification and Eligibility Interactions

Type of Architecture	Type of Interaction	FDSH ID	Interaction
Medicaid/CHIP (M&C) agencies in FFE states, SPE, SBE States	Enrollment & Reconciliation	H20	*HIPAA 834 Enrollment
		H35	Transfer Recon Discrepancy Reports
		H36	*Exchange Generation of Monthly and 1095 End-of-Year Reporting to IRS (monthly file)
		H41	*Exchange Generation of Monthly and 1095 End-of-Year Reporting to IRS (annual file)
	Verifications	H01	Remote Identity Proofing
		H03	SSA Composite Service
		H04	Verify Lawful Presence Service (VLP)
		H05	VLP Send Documents
		H06	VLP Mailed Documents
		H07	VLP Closed Case
		H08B, H08T	Current Income
		H09B, H09T	Annual Income
		H14	**Verify Employer-Sponsored-Insurance (ESI) Minimum Essential Coverage (MEC)
		H43	Quarterly Eligibility Verification
		H48	VLP Retrieve Resolution
		H53	VLP Get Case Details

* - Not required for Medicaid and CHIP
** - Federal Employee Health Benefits Program

4.2 STATE-SPECIFIC INTERACTIONS FOR MEDICAID/CHIP AGENCIES IN FFE STATES

The table of “State-specific interactions for Medicaid/CHIP Agencies in FFE States” provides a list of interactions with the FDSH that are unique to Medicaid/CHIP Agencies in FFE States. This list allows the reader/tester to understand the scope of interactions. These interactions may be real-time services or batch processed data exchanges. The data exchange model applicable to each interaction is provided in the State Testing Profile at the time they are distributed to each State.

Note: All services listed were confirmed as of 02/22/2013. For most recent list of services search for “service forecast” on CALT (https://calt.cms.gov)

Table 3 - State-Specific Interactions for Medicaid/CHIP Agencies in FFE States

Type of Architecture	Type of Interaction	FDSH ID	Interaction
Medicaid/CHIP Agencies in FFE States	M&C Integration	H15	Account Transfer
	Verifications	H31	*Non-Employee Sponsored Insurance Minimal Essential Coverage

* - MEC check for current Medicaid & CHIP; real-time during application and batch in quarterly enrollment (FFE invoking the service via the FDSH to get to M&C)

In addition to the FFE-specific FDSH interactions it is important to note that the FFE solution will be implemented as a multi-tenant solution, each tenant being an individual instance of an FFE. It will offer a pre-determined set of configuration options for CMS to use in customizing the business rules and User Interface (UI) themes and branding, where appropriate, for each FFE State. The various customization and configuration options anticipated include;

- User Interface Themes and Branding: customization options available with instructions for how state-specific branding will be applied to the FFE.
- Medicaid Rules for the FFE: customizable elements of eligibility rules for M&C (described in September 2012 CMS guidance, available on CALT)
- Connection to each FFE State’s Medicaid / CHIP Enrollment Records
- A unique test profile and electronic account transfer for Medicaid/CHIP agencies choosin to not utilize IRS data

Note: As of this release (ver. 1.0) of the Testing Handbook these configuration options have not been finalized. They will be added to an appendix or referenced when available.

4.3 STATE-SPECIFIC INTERACTIONS FOR SBE

The table of State-specific interactions for SBE provides a list of interactions with the FDSH that are unique to SBE State's. This list allows the reader/tester to understand the scope of interactions which may be real-time services or batch processed data exchanges. The data exchange model applicable to each interaction is provided in the State Testing Profile at the time it is distributed to each State.

Note: All services listed were confirmed as of 02/22/2013. For most recent list of services search for "service forecast" on CALT (https://calt.cms.gov)

Table 4 - State-Specific Interactions for SBE

Type of Architecture	Type of Interaction	FDSH ID	Interaction
SBE States	State Based Exchanges	H10	Appeals
		H46	Current QHP Enrollment/APTC Check
	Enrollment & Reconciliation	H34	Transfer Recon File Received in 834 Format
	Federal Functions	H19B, H19T	Advance Payment Computation
	Verifications	H31	**Non-Employee Sponsored Insurance Minimal Essential Coverage

** - All MEC verifications except for M&C

4.4 DATA EXCHANGE PATTERNS AND PROTOCOLS

The SBEs, M&C agencies, Issuer systems and the FFE will interact with the FDSH, which provides common business services and interfaces to Federal agency information. Various systems operated by these stakeholders will utilize the business services offered by the FDSH to request information from, or provide information to the States. The technical architecture of the FDSH is designed to accommodate data exchange via service based communications as well as through batch file transfer mechanisms.

The FDSH services will be invoked across the web over the HTTP protocol. Web service will be invoked using Extensible Markup Language (XML)/Simple Object Access Protocol (SOAP) messages, which will be predefined in Web Services Description Language (WSDL) documents. Systems consuming services will be able to exchange XML messages in two (2) distinct modes:

- Synchronous (real-time) and
- Asynchronous (deferred or delayed).

The availability of the data exchange mode(s) will be specified by CMS. A State's capability to accommodate these different types of service connection and delivery modes will be captured within the State Testing Profile. State preferences will be captured in order to prepare appropriate test cases that take into consideration alternate methods of transfer if primary means are unavailable (asynchronous in place of synchronous, for ex.). See **Appendix C – Data Exchange Patterns and Protocols** for a detailed explanation.

Batch processing (i.e., executing a series of non-interactive jobs all at one time) will also be available through the FDSH for select interactions. Batch jobs can be held during working hours and then executed during the evening or when the system is idle or "quiet." Batch processing is particularly useful for operations that require the system or one of the system's peripheral devices for an extended period of time. Once a batch job begins, it continues until it is done or until an error occurs. Note that batch processing implies that there is no interaction with the user for the subject operations or transactions while the program is being executed.

5 TEST SCENARIOS, CASES AND DATA

In an effort to support State testing, CMS will furnish test data for States to utilize in their various testing efforts. This section discusses how the FEPS test scenarios, cases and data are built, how to access the material and how they will be utilized.

5.1 TEST SCENARIOS AND CASES

In order for States to be able to test their systems comprehensively, CMS has developed a logic-based approach to FEPS testing. CMS will build FEPS test scenarios comprised of a sizeable number of business logic conditions that can be converted into one or more test cases. FEPS tets scenarios will be developed to cover single data request and retrieval transactions as well as multiple interactions with States and Federal partners. FEPS test cases and data will be created to capture all the interactions and business logic associated with each scenario.

FEPS test scenarios follow two approaches.

- **The top-down approach**: develops business cases that attempt to cover a range of options. The scenarios are then converted into test cases by assigning the necessary values to each data element.
- **The bottom-up approach:** develops scenarios by creating matrices that include all possible combinations of key data elements and their values. Some of the values will be straightforward, gender equals either male or female. Other data will vary, such as the income as percent of Federal Poverty Level (FPL). When using the bottom-up approach, the scenarios can perform two functions;
    - ➢ Identify which elements must vary and how they must vary. Thus, the household model indicates that there are four types of filing status that must exist within the test data.
    - ➢ Confirm that test cases cover all possible combinations of data.

Additionally, with these FEPS scenarios, States are expected to verify that all system outcomes are performing as expected even given scenarios built to exercise boundary conditions, null results, and failure modes. Boundary conditions will test the maximum and minimum values as well as values that are just outside the accepted range. Null results and failure modes will test whether a system can identify error values and process accordingly.

In addition to these CMS-developed scenarios for FEPS testing, CMS will also collaborate with States to identify and accommodate other possible test scenarios that require FEPS and State Integration-based business, operational or other gate review requirements, such as the Blueprint Test Scenarios.

Once the State Testing Profile has been documented, appropriate test scenarios will be identified by the FEPS Independent Test Team based on interactions that befit each State involved in a test type execution phase. Once the proposed FEPS scenarios have been agreed upon by CMS and the State(s), CMS will load FEPS test cases and data into CALT based on each of the FEPS scenarios and make it available to the States. Note that Blueprint Test Scenarios are also available on SERVIS.

5.2 TEST DATA

FEPS test scenarios, cases and data will be made available to the States by contacting their respective OIS IT PMs or State Medicaid E&E Systems Analysts. It is also anticipated that the cases and data will be made available within the CALT tool at https://calt.cms.gov/sf/docman/do/listDocuments/projects.se_portal_sandbox/docman.root.testing

To generate the test data, CMS will use both manually and randomly generated data to populate the individual test cases to meet all required boundary and negative testing conditions. Generating test cases requires close coordination with specific Federal agencies, including SSA, IRS, and DHS, to provide certain critical data elements needed to create integrated test cases. SSA and DHS will provide unique identification information that CMS will integrate into the shared library of test data. IRS will incorporate those unique identifiers into their own test data bed of income information and share those data elements with the CMS library of test data. Additional coordination with other Federal agencies such as Veterans Affairs, TRICARE, Office of Personnel Management, and Peace Corps are expected to begin soon. Once the shared library of test cases is complete, CMS will auto-generate any additional data needed to test the system. All test data will be generated in a logical, structured manner that conforms to FEPS business rules.

The test data will be provided in Microsoft Excel format. The data is designed to populate either a test tool that simulates access to the States systems or the user interface/application that is planned to provide the functional mechanism to issue FDSH requests as well as receive responses under appropriate test cases. FEPS test scenarios, test cases and data will be available in CALT at

CMS State Testing Handbook, ver.1.0

https://calt.cms.gov/sf/docman/do/listDocuments/projects.se_portal_sandbox/docman.root.testing

States will coordinate with their OIS IT PMs or Medicaid E&E Systems Analysts, who will assist with organizing test execution for each of the test type phases that are included in the State's FEPS-and-Partner Test Plan. CMS will utilize an FEPS Independent Test Team who will prepare FEPS test scenarios, cases and data packages for each State partner. The test data will also include "expected results" and outcomes aligned with the test cases. This comparison process of outcomes will have both automated and manual validation with iterative review in a multi-step testing process (see section 6.4).

6 TESTING PROCESS

The State FEPS-and-Partner Testing model is based primarily upon scenarios created to cover all logical workflow paths attributed to State functional interactions. Furthermore, scenarios include test cases and test data that will validate the correct implementation of the approved BSDs, ICDs, data exchange method and supporting system transaction and processing functionality. The CALT library of ICDs, BSDs, etc. will link to applicable test scenarios, test cases, and test data. This will permit the State tester to quickly identify which test scenarios, cases, and data are best suited to meet the needs of the particular test type or configuration item being tested.

During the test preparation period, after the State Testing Profile information has been captured, a detailed FEPS-and-Partner Test Plan and Schedule that defines the test scenarios and cases to be executed will be developed by the FEPS Independent Test Team. The FEPS-and-Partner Test Plan will also prioritize the tests to be performed, identify the parties responsible for support and coordination, outline expectations around information assembly and reporting and include the appropriate templates for documentation and repositories for storing those documents.

6.1 TEST EXECUTION ROLES AND RESPONSIBILITIES

FEPS-and-Partner testing requires significant coordination and communication between different CMS entities as well as contractor support. Table 5 identifies the primary FEPS points of contact by testing activity. Individual POCs for the contact organizations listed will be provided as part of the Introduction, Orientation and Onboarding activities for each Wave testing period. Under any circumstance where an individual is not named for a testing activity the OIS IT PM or Medicaid E&E Systems Analyst will be able to assist with locating a Subject Matter Expert.

Table 5 - Points of Contact by Testing Activity

Testing Activity	Points of Contact

Pre-qualification	• OIS IT PM for SBE States* • Medicaid E&E Systems Analyst for FFE/SPE States* • CIISG State Engagement Team
Introduction, Orientation and Onboarding (Testing Package distribution, training webinars, walkthroughs)	• CIISG State Engagement Team* • OIS IT PM for SBE States • Medicaid E&E Systems Analyst for FFE/SPE States • RTS • FEPS Independent Test Team • CIIO State Exchange Group • FFE/SPE State Onboarding Team
State Profile Collection	• OIS IT PM for SBE States* • Medicaid E&E Systems Analyst for FFE/SPE States* • RTS • FEPS Independent Test Team • CCIIO State Exchange Group • FFE/SPE State Onboarding Team
Communicate FEPS-and-Partner Test Plan, Test Scenarios, Test Cases and Test Data	• OIS IT PM for SBE States* • Medicaid E&E Systems Analyst for FFE/SPE States* • FEPS Independent Test Team • CIISG State Engagement Team • CCIIO State Exchange Group • FFE/SPE State Onboarding Team
Test Readiness Review	• FEPS Independent Test Team* • RTS* • OIS IT PM for SBE States* • Medicaid E&E Systems Analyst for FFE/SPE States* • CIISG State Engagement Team • CCIIO State Exchange Group • FFE/SPE State Onboarding Team

Test Execution	• FEPS Independent Test Team* • OIS IT PM for SBE States • Medicaid E&E Systems Analyst for FFE/SPE States • RTS
Testing Support - Defect Tracking	Exchange Operations Support Center CMS_FEPS@CMS.HHS.Gov 1-855-CMS-1515

* - Lead

6.1 TEST READINESS REVIEW (TRR) CHECKLIST

CMS will hold joint Test Readiness Review (TRR) meetings with all relevant stakeholders affiliated with the State prior to beginning the actual test execution for each Test Type. Each TRR will result in a testing "Go/No-Go" decision based on a jointly-defined checklist of required criteria. A sample of the TRR Procedures and Checklist is provided in **Appendix D – TRR Procedures and Checklist.**

6.2 TEST TOOLS

The list of Test Tools identified in Table 6 has been provided for informational reference only. States are not required to use any of these tools but may choose to consider this set as these will be used by the FEPS environment during test execution and common tools will likely ease any technical or configuration burdens.

Table 6 - Test Tools

Test Tool	Purpose
SoapUI Pro	FDSH Testing
CALT	Overall tracking and requirements/Test Cases/defects management
Quick Test Professional (QTP)	Functional automated test script execution/regression
LoadRunner	Performance/stress testing
BrowserStack	Cross browser testing

6.3 SECURE COMMUNICATIONS TEST

The secure communications test which will enable the FEPS-and-Partner web service testing involves a network ping to check whether either side has the communication ports/protocols open for future testing. At a minimum, the following steps and exchange of information are required:

1. *State* will share the Public IP address of the gateway and port listened on for the services with the *OIS IT PMs or Medicaid E&E Systems Analysts* who will provide the information to *Regional Technical Support (RTS)*
2. *State* will request the same from *RTS* for the FEPS environment configuration

Additional detail pertaining to the secure communication test type will be contained within the State's FEPS-and-Partner Test Plan. To conduct the communications test in a secure manner the *State* should follow these steps to request a FDSH certificate:

1. Send an email to the FDSH Security group (FDSHSecurity@qssinc.com) to obtain the following:
   a. User ID and Password to be used in the WSSE header
   b. Primary and Secondary VeriSign certificates
   c. The public key for the FDSH Gateway
   d. End points secured by the SOA Gateway on the Test Environment
2. Provide the following information in the email:
   a. Name
   b. Organization Name (e.g., ABCD Corp
   c. Organization Unit (e.g., FDSH, FFE, SBE, SPE, Medicaid/CHIP, etc.)
   d. Agency Name (e.g. Washington State Health Care Authority)
   e. Email address
   f. Telephone Number
   g. Attach the certificate file (Note: The email server does not accept attachments with the .cer extension. Copy your alias.cer file to alias.txt and attach the alias.txt file. If your organization has a trusted CA issued certificate, copy your trusted .cer file to alias.txt and attach the alias.txt file.)
3. Within 2 business days, you will receive a response from the FDSH Security group with the following details:
   a. User ID to be used in the WSSE header
   b. End points to be used in the soapUI test
   c. An attached zip file, which will include the following:
      i. Primary and Secondary VeriSign certificates
      ii. The public key for the FDSH gateway
4. A second email will follow with the password. After unzipping, save the certificates to a folder from which commands were run (i.e. current working directory).
5. Use information received to build the key store and configure soapUI.

6.4 FEPS-AND-PARTNER

The FEPS-and-Partner testing which includes the invocation of FDSH Secure Services via the State's systems (UI/application or database) requires the following steps and exchange of information, at a minimum:

1. *Regional Technical Support* will exchange the sample service details: WSDL, endpoints, port numbers, IP Address of the communication gateway.
2. *Regional Technical Support* will exchange the security certificates issued by a third party
3. Once details are received from the respective *State* a Firewall Request is opened with the Host Provider (Terremark) through a request from RTS to allow communication to the *State*.
    a. This requires an approval from CMS Security Team to execute the firewall request
    b. At the same time similar setup might be needed on the State side as well

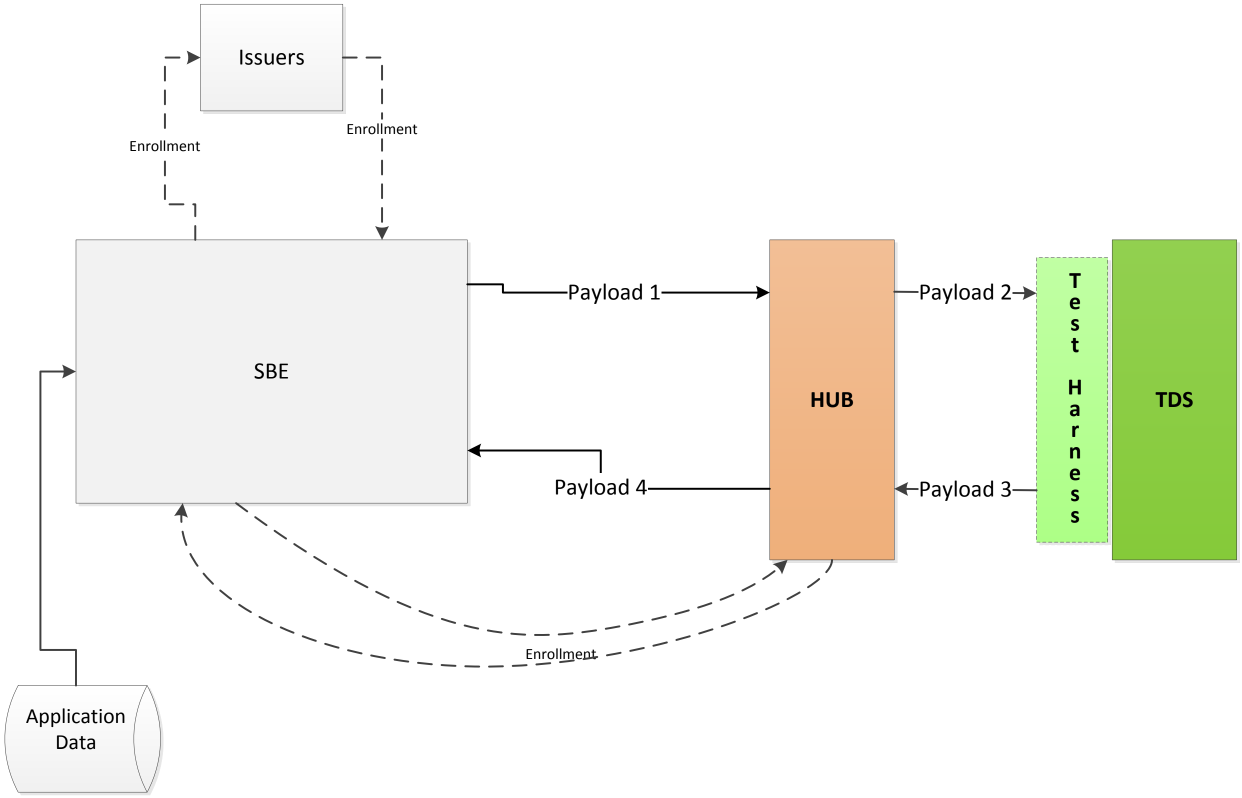
FEPS-and-Partner testing, including the test scenarios, cases and data will follow a pattern that is distinguished by the type of State organization that is communicating with the FDSH as well as the origination of the initial application.

In the model represented in Figure 1 State-Based Exchanges and M&C Agencies will be provided with “application” test data by the respective OIS IT PMs, Medicaid E&E System Analysts or the FEPS Independent Test Team that meets with all the logistical constructs for the FDSH interactions to be tested. The data will be provided in the form of an “application” suitable for the State to ingest into their UI/application “system(s)”. From that point on the validated test results are focused upon Payload 1 and Payload 4 transactions to answer these essential questions:

1. Can the State generate correct Payload 1 requests to FEPS?
2. Were the requests in the correct sequence that meets with the desired results of a broader Test Scenario?

Payload 1 is captured and the actual results are compared to the expected results by the FEPS Independent Testing Team for verification The transactions between the FDSH and the Test Harness that represents connectivity to the Trusted Data Sources (TDS), Payloads 2 & 3, are not a part of the validated connections and transactions. These transactions have been verified prior to FEPS-and-Partner test execution through internal testing. The States will also be required to consume and process the response, Payload 4. Results of Payload 4 consumption will be verified by the State’s IV&V contractor and reported to the State IT PMs or Medicaid E&E Systems Analysts.

Figure 1 - SBE to FEPS Testing Pattern



In the model represented in Figure 2, Medicaid and CHIP Agencies will be provided with "application" data that meets with all the logistical constructs for the FDSH interactions to be tested. The data is provided in the form of an "application" suitable for the Agency Partner to ingest into their UI/application "system(s)". From that point on the validated test results are focused upon Payload 1 and Payload 4 transactions to answer these essential questions:

- Can the Agency generate accurate Payload 1 requests to FEPS?
- Were the requests in the correct sequence that meets with the desired results of a broader Test Scenario?

Payload 1 is captured and the actual results are compared to the expected results by the FEPS Independent Testing Team for verification. The transactions between the FDSH and the Test Harness that represents connectivity to the Trusted Data Sources (TDS), Payloads 2 & 3, are not a part of the validated connections and transactions. These transactions have been verified prior to Test Execution through internal testing. The Agencies will also be required to consume and process the response, Payload 4. Results of Payload 4 consumption will be verified by the State's

IV&V contractor and reported to the OIS IT PM or Medicaid E&E Systems Analyst for confirmation of test completion.

Figure 2 - Medicaid and CHIP to FEPS Testing Pattern

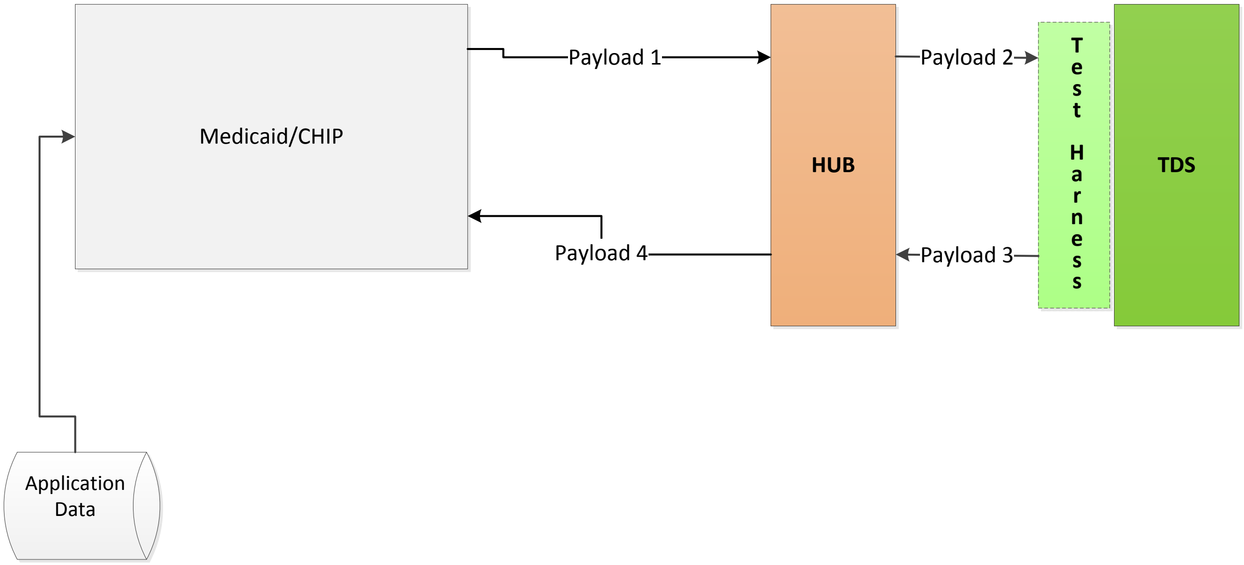
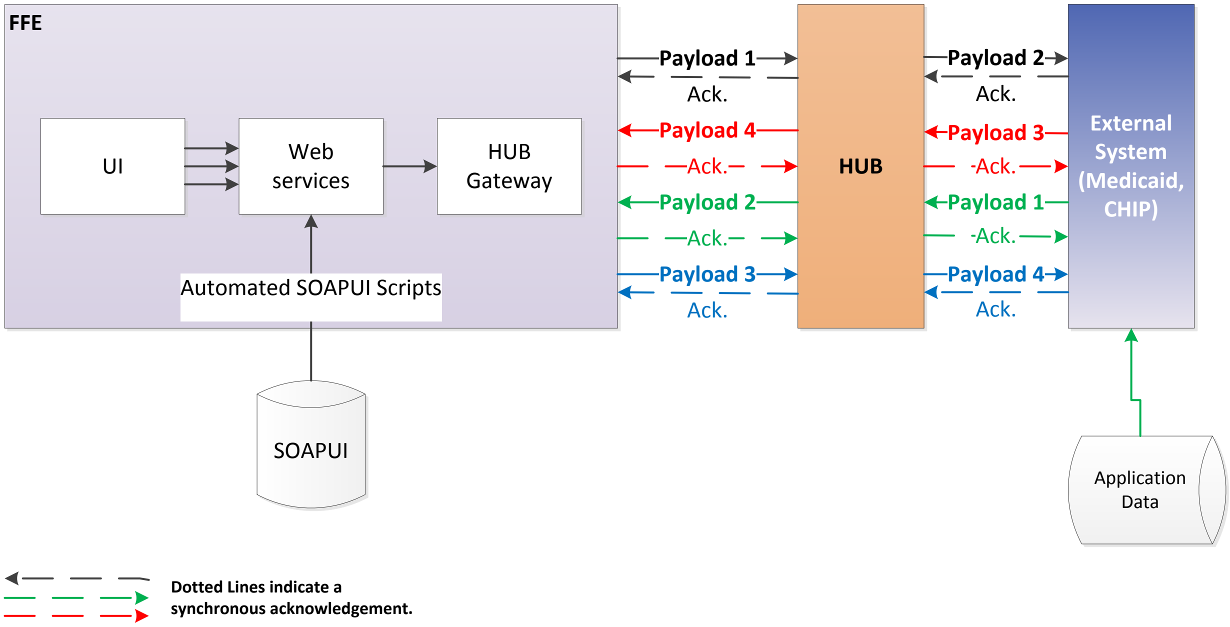


Figure 3 represents a unique Medicaid/CHIP type of transfer to/from the FFE. The graphic shows an account transfer originating from the FFE as well as the State's Medicaid/CHIP system. As in Figure 1 the payloads being tested and verified include Payload 1 & 4 depending upon where the initial request originates from.

Figure 3 - FFE or Medicaid/CHIP Initiated Transfer Testing Pattern



Additional detail pertaining to the FEPS-and-Partner test type will be contained within the State's FEPS-and-Partner Test Plan.

6.5 TEST VALIDATION

Secure communication tests will include two ping tests between CMS and States. The initial ping test verifies that systems participating in the interface can communicate with each other at the network layer. The second ping test verifies that the systems can communicate securely at the application layer.

FEPS-and-Partner test results will be verified through use of the following methods:

- Demonstration - Observable functional operation
- Testing - Relies on special test equipment or instrumentation
- Analysis - Interpretation or extrapolation of test results
- Inspection - Examination of interfacing entities, documentation, etc.

CMS and States will employ the testing and analysis qualification methods to validate compliance with requirements. The testing qualification method includes evaluating and executing test scenarios under controlled conditions, configurations, and inputs in order to observe the responses from the FDSH. This is represented as "Payload 4" in **Figure *1***.

The analysis qualification method includes quantifying and analyzing test results to determine if services have been developed based upon the required BSD specifications. This is represented as “Payload 1” in **Figure *1***.

For the FEPS-and-Partner transactions that are tested;

- Application data will be provided to the States by the *OIS IT PMs, Medicaid E&E Systems Analysts or FEPS Independent Test Team* as well as payload 4
- The *FEPS Independent Test Team* verifies payload 1 is created correctly by the State by comparing the actual “payload 1” to expected results “payload 1”
- The State’s *System Integrator* or *IV&V Contractor* verifies that they can consume Payload 4. The System integrator may be involved in the process prior to actual verification. Once the expectation for testing includes verification the IV&V contractor becomes involved
- If there is believed to be a testing defect or erroneous result the procedures described in section 7, Defect Management, should be followed.

FEPS-and-Partner transaction testing includes the identification of expected outcomes, creation of payload from application data provided by CMS, determination and validation of output based on the specifications, test scenario execution and the comparison of actual and expected outputs. Testing scenarios will include positive and negative scenarios to verify systems correctly process data when data is correct and incorrect. CMS and States will agree on the procedures and data to be collected for each test and agree on specific criteria for success and failure.

6.6 TEST REPORTING

Test reporting is the essential capture of the input and characterization of the testing steps measured against the results and status. The report provides a view into the State’s progression status of testing and insight into what is causing any issues or problems by an individual State as well as in a collection of multiple States involved in a particular Wave. The reports are generated by the State on a weekly basis and will be made available to the State’s IT PM or Medicaid E&E Systems Analyst.

A Weekly Test Status Report will be produced that contains, at a minimum, the following details:

- Total number of Test Cases in the inventory
- Number of Test Cases planned to be executed
- Number of Test Cases executed
- Number of Test Cases passed
- Number of Test Cases failed
- Number of Test Cases not run, deferred, and/or waived
- Number of new defects reported with subtotals for each Severity Level

- Number of new defects closed with subtotals for each Severity Level
- Total number of defects remaining open with subtotals for each Severity Level
- Total number of defects closed with subtotals for each Severity Level

CMS provides a Test Summary Report template which can be modified to a State's criteria: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/TestSummaryRpt.zip

7 DEFECT MANAGEMENT

The validation of FEPS-and-Partner test cases will be the responsibility of the FEPS Independent Test Team and the State's IV&V contractor. The characterization of "defects" within FEPS-and-Partner testing includes system issues, testing problems as well as discrepancies between actual and expected results.

A record of a defect must be created to document any condition that occurs during testing where the expected result for a test step does not match the actual result. The record can be logged via email, phone or through a web interface, described in section 7.1. A severity level and priority is designated during the FEPS Defect Management workflow as described in in section 7.1. Responsibility for troubleshooting and resolution is assigned to the appropriate area of FEPS operations by the triage specialists within the Exchange Operations Support Center (XOSC) Help Desk.

Severity levels are translated as follows to better represent the impact placed upon testing:

Severity	Description	Example
S1- Critical	The defect is a "showstopper" which means that operational functions, mission critical functions, and testing activities cannot be performed.	The Internet browser no longer displays the system, but a "Server 500" error or a "400" error instead.
S2 – Severe	The defect impacts operations and / or degrades functionality; however, a workaround is available such that testing may still be performed.	Data cannot be submitted from one entry point in the system, but an alternate entry point exists
S3 – Moderate	The defect indicates a requirement is not met; however, the defect does not hinder mission critical functions, operations, or testing. Further, if the defect was NOT corrected an end user could still perform the functions of the system without adverse impact.	The system doesn't have a print button, but the internet browser can be used to print.
S4 – Irritant	Results in user / operator inconvenience or annoyance, but does not affect a required operational or mission essential capability.	A button is hard to find on the page.

S5 - Documentation / Process	Any defect that requires a documentation change to correct (e.g. user stories, blueprints, etc.)	The test case says click on the "Enter" button but the system's label is "Ok".

As part of the Defect Management workflow all defects are reviewed by the XOSC triage specialists to determine the appropriate course of action based on the severity and priority of the issue. Available courses of action include:

- Fix immediately
- Defer fixing until a later release date
- Close defect without applying a fix. A defect record may be closed without a fix under the following circumstances:
  - ➢ The issue is not within the scope of the current requirements. In this case an enhancement request may be generated.
  - ➢ The same issue was already documented in another defect. In this case, it is logged as a duplicate defect and associated with the initial defect.
  - ➢ Other circumstances, as defined by the FEPS Independent Test Team

Defects that are not anticipated to be closed immediately will be scheduled to be fixed and placed into a queue for the Development Team to address. On both a scheduled and emergency basis, new application releases incorporating fixes will be verified internally and then moved into the external test environment. If the State is still within their test execution period they will re-test the area affected by the defect. If the test execution period has concluded they may re-test in the next Wave if available, within the informal test environment or as part of future End-to-End testing.

In addition to application functionality defects, issues impacting testing operations will be logged through the Defect Management process. Examples of these types of issues include an inability to access the test environment due to incorrect usernames, passwords, or user roles. Logging will allow for the appropriate escalation of issues, highest visibility, and ability to track to closure.

7.1 DEFECT MANAGEMENT WORKFLOW

- States who uncover a defect, must log the defect with the XOSC Help Desk. Options include;
  - ➢ Email: CMS_FEPS@CMS.HHS.Gov
  - ➢ Phone: 1-855-CMS-1515
  - ➢ Web(***future***): CALT is integrated with the trouble ticket system and a defect can be reported through a CALT interface (***future***) to report a problem

- The Help Desk opens up a trouble ticket; performs an initial triage and sends the defect to the appropriate FEPS operational team to further analyze and troubleshoot (FDSH & FFE contractors as well as the Independent Testing Team)
- The recipient team has the responsibility of verifying the initial severity and priority ratings and determining the appropriate course of action regarding repair.
- The primary means of status checking is driven by the submitter who can contact the XOSC or visit the CALT interface to Remedy and search on the Remedy ID (***future***)
- Resolution response is coordinated through Regional Technical Support and the State's OIS IT PM or Medicaid E&E Systems Analyst

7.2 TRACKING DEFECTS

The information pertaining to the issue will be captured in the XOSC trouble ticket system. When a tester encounters a defect, testing should continue for the remaining steps of the test case (if possible), and all subsequent defects will be logged.

As defects are identified during testing, they are initially recorded in the XOSC trouble ticket system and then moved to the defect management system of the FEPS Operational team that is assigned ownership. Defect management reports are built through a joint defect tracking spreadsheet. The details of the data collected are shown in Table 9 – Defect Tracking Data.

Table 7 - Defect Tracking Data

Data Element	Description
Date Identified	Date of test
Test Case Identifier	Identifier from Test Case
Test Steps Causing Defect (e.g., step numbers)	Step number from Test Case
Test Phase	Wave and Test Type
CMS Defect Identifier	Identifier filled in for CMS-reported defects
State Defect Identifier	Identifier filled in for State-reported defects
Status	Current defect State (open, closed, deferred)
Escalation	If a defect cannot be resolved, identify to whom it has been escalated
CMS Version Number	Identification number for the CMS system that was being tested
State Version Number	Identification number for the State system that was being tested
Defect Title	Name of the defect
Defect Description (Brief)/Symptoms	A description of the defect and the symptoms exhibited

Defect Severity	The severity of the defect; the severity level indicates the degree to which the defect identified impedes system operations (S1 – Critical, S2 – Severe, S3 – Moderate, S4 – Irritant, S5 – Documentation //Process)
Defect Priority	The priority of the defect; the priority level indicates the relative importance of repairing the defect. A defect with a high priority (irrespective of its severity level) will be fixed. (P1 – Urgent, P2 – High, P3 – Medium, P4 – Low)
Defect Source	Where the defect was ultimately injected into the system
Estimated Repair Date (Version)	Date that the repair will be corrected; version containing repair
Notes	Any notes or comments about the defect

7.3 EVALUATING AND RE-TESTING DEFECTS

Defects will be evaluated by the FEPS Program/Development Management team and may result in updating the application to address the issue. Eventually, the updates will be moved into the test environment, and the State tester will be asked to execute the steps again to verify that the issue has been successfully resolved.

The FEPS Program Management team may decide to "defer" a defect fix depending on the nature and severity of the defect. In this situation the tester may complete their assignment with test cases that are still in the "Failed" State. It is feasible that a tester may be contacted after the testing phase to assist with the validation of a software refinement to resolve a "Failed" test case.

8 WAVE 1 TESTING TIMELINE AND KEY DATES OVERVIEW

The following phases, timeframes and key dates are associated with the Wave 1 State Testing Lifecycle.

8.1 ESTIMATED TIMELINE FOR STATES PARTICIPATING IN WAVE 1

Table 8 - Timeline of Key Activities for Wave 1

Phase	Timeframe	Key Activities

Information Gathering	Feb. – March 2013	• Completion of State Testing Profile • Finalization of State FEPS-and-Partner Test Plan and Schedule • Test Scenarios and Cases are drafted, shared and reviewed
Test Preparation	March 2013	• CMS Test Data shared with the States • Conduct Test Readiness Review (TRR) for formal test entrance • Environments and security requirements (if applicable) are managed and verified • Populate State UI/Application Systems with Test Data
Test Execution	March – April 2013	• Conduct Secure Communications Test • Conduct FEPS-and-Partner Integration Testing
Test Exit Criteria and Documentation	March – April 2013	• Defect tracking, verification and reporting of results • Exit criteria is reviewed • Create Security Testing Results Report • Create Defect Tracking Report • Create Test Summary Report

8.2 KEY DATES FOR SBE STATES

State Based Exchanges have milestones that are based upon the FEPS Formal Testing model and include:

- May 1, 2013: Last date to enter FEPS-and-Partner Formal Testing
- June 1, 2013: CIISG provides and assessment report to CCIIO based upon the reported results of FEPS-and-Partner Formal Testing
- July 1, 2013: CCIIO produces the results of the formal determination of a SBE

More details are forthcoming on FFE/SPE testing milestones.

Appendix A – Acronyms

BSD	Business Service Descriptions
CALT	Collaborative Application Lifecycle Management Tool
CCIIO	Center For Consumer Information and Insurance Oversight
CHIP	Children's Health Insurance Program
CIISG	Consumer Information & Insurance Systems Group
CMCS	Center for Medicaid and CHIP Services
CMS	Centers for Medicare & Medicaid Services
CSV	Comma Separated Value(s)
DHS	Department of Homeland Security
EDI	Electronic Data Interchange
EPR	Endpoint Reference
FDSH	Federal Data Services Hub
FEPS	Federal Exchange Program System
FFE	Federally-Facilitated Exchange
FPL	Federal Poverty Level
FTP	File Transfer Protocol
HHS	Department of Health and Human Services
ICD	Interface Control Documents
IPT	Integrated Project Team
IRS	Internal Revenue Service
RTS	Regional Technical Support
SBE	State Based Exchange
SHOP	Small Business Health Option Program
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SPE	State Partnership Exchange
TDS	Trusted Data Source
TRR	Test Readiness Review
WSDL	Web Services Description Language

XML	Extensible Markup Language
XOSC	Exchange Operations Support Center

Appendix B – Reference Documents

Current

- **Onboarding Guide to the Federal Data Services Hub, v1.1 (“Hub”)**

  https://calt.cms.gov/sf/go/doc19688?nav=1

  The Onboarding Guide has been written to provide States and other integration partners with an understanding of the basic functions of the Hub. The Guide discusses Hub integration partners, basic Hub testing concepts, and resources available for IT developers. The guide provides a high-level description of the onboarding process, including an overview of the necessary information to connect to the Hub and make use of Hub-provided services.

Planned

- **Technical Guide to the FFE and Technical Guide to the Hub**

  (CALT location forthcoming)

  The Technical Guides to the FFE and the Hub may be restructured to align with specific user groups. Currently planned are CMS Exchange Systems Communications User Guides for Issuers, States participating in the FFE or SPE, SBEs, and State Medicaid and CHIP agencies as well as a CMS Exchange Systems Overview, a Hub Connections Reference Manual, and a Hub Services Reference Manual, Together these provide comprehensive documentation of the FFE and Hub architecture and capabilities as well as CMS documentation repositories available to support Exchange implementation or integration with CMS systems.

Appendix C - Data Exchange Patterns and Protocols

The Service-based Data Exchange Model uses the four data exchange patterns described as follows. States will select the pattern that best integrates with their infrastructure and test with the FDSH using that pattern.

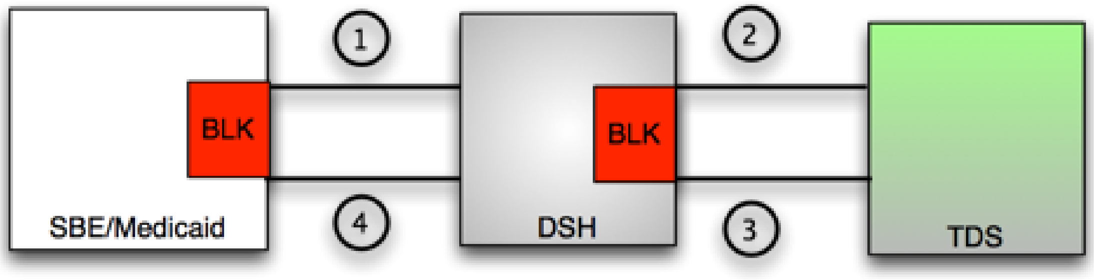
Interaction Notes:

Web services are defined as synchronous (sync) or asynchronous (async) at the time of design.

- If a synchronous web service is invoked and the Trusted Data Source (TDS) system is down or unavailable, the FDSH will send an error response to the requestor (e.g. the State Medicaid System).
- If an asynchronous service is invoked and the TDS system is down, the FDSH will queue the incoming requests and process them in a "First in First Out" (FIFO) model once the TDS is up. The FDSH will then call back with the responses (async with call back) or respond to requests (async with pull) with error messages until TDS has processed the requests.
- In the first version FDSH will not support the model of a single service in both synchronous and asynchronous mode.

Synchronous Communication Data Exchange Pattern

Synchronous services can be characterized by the State client invoking a service and then waiting for a response to the request. Because the client suspends its own processing after making its service request, synchronous services are suited to scenarios when the service can process the request in a small amount of time. Synchronous services are also best when applications require a more immediate response to a request. Whenever the FDSH can provide near real-time verifications, it will expose them through synchronous services, allowing the consumer to obtain results from verification in single message exchange (request/response).



Steps:

1. A SBE/Medicaid/CHIP E&E System opens a communication channel to invoke a web service on the FDSH. The SBE/Medicaid System is blocked until the web service makes a response on the same communication channel (HTTP Tunnel).

2. The FDSH processes the incoming request and initiates a service request to the appropriate Trusted Data Source (TDS) in a synchronous manner. The FDSH then waits for the service request response from the TDS.

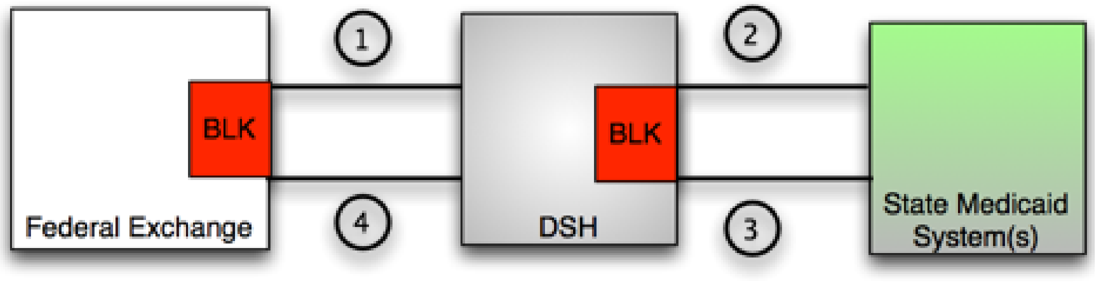
3. After receiving the response from the TDS, the FDSH processes the response to the requestor/client and closes the tunnel.

Exceptions

1. At any time, if the connection is lost the request is lost and there is no recovery.
2. The FDSH triggers a timeout error if the TDS is not responding to the request within the Service Level Agreement (SLA) threshold. The timeout error is communicated as an error message back to the requestor /client entity.

Reverse Synchronous Communication Data Exchange Pattern

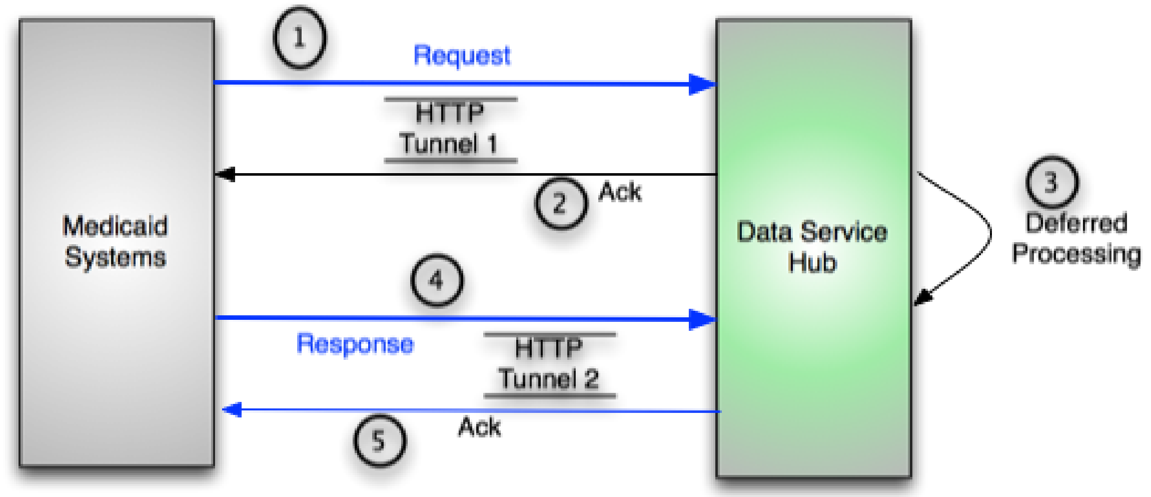
The only difference from the previous pattern is that the State Medicaid System acts as a data source in this pattern. All the above concepts apply.



Asynchronous Communication Data Exchange Pattern with Call Back Mechanism

With asynchronous services, the State client invokes the service, the FDSH acknowledges the receipt, but the actual response from processing of the request is sent to the client in a call-back from the FDSH (deferred response). Whenever the FDSH cannot provide near real-time verifications, it will expose them through asynchronous services with a deferred response.

For all deferred responses, clients will have to host a callback service that the FDSH will call to submit the results from processing. The actual response times for deferred services will vary from service to service, and they will be described in the SLA's that the FDSH will publish in the CMS Service Repository (WS Repository).



Steps:

1. SBE/Medicaid system invokes the web service request to the FDSH in an asynchronous manner.

2. FDSH then accepts the request and generates an acknowledgement of the request. (The acknowledgement step is optional).

3. FDSH internally starts processing the request. This internal processing may require invoking additional web services that may or may not be asynchronous.

   SBE/Medicaid System has an option of:
   - Opening a communication channel (HTTP port/socket) without a defined WSDL, or
   - Using a web service and managing all of the SOAP-related issues. In that case, it does not matter what comes in on the socket, the SBE/Medicaid System would be able to take the message and process it. But the complexities of the message would have to be managed by the SBE/Medicaid System explicitly in the code.

4. Alternately the SBE/Medicaid System can expose a web service to take the response from FDSH. **(Recommended)** This would enable an Endpoint Reference (EPR) to be created. This is the call-back mechanism where the SBE/Medicaid System will write a second service that has an operation of only receiving and processing the response. The SBE/Medicaid System generates an acknowledgement for the receipt of the response.

5. Please note that the ability of the SBE/Medicaid System to relate the response to the original request is based on the following:

Correlation ID: It will be embedded in the content of the web service for the processing on the SBE/Medicaid side
WS Reliable Addressing: This defines the following keep attributes such as TO, Action, Message ID and Reply to.

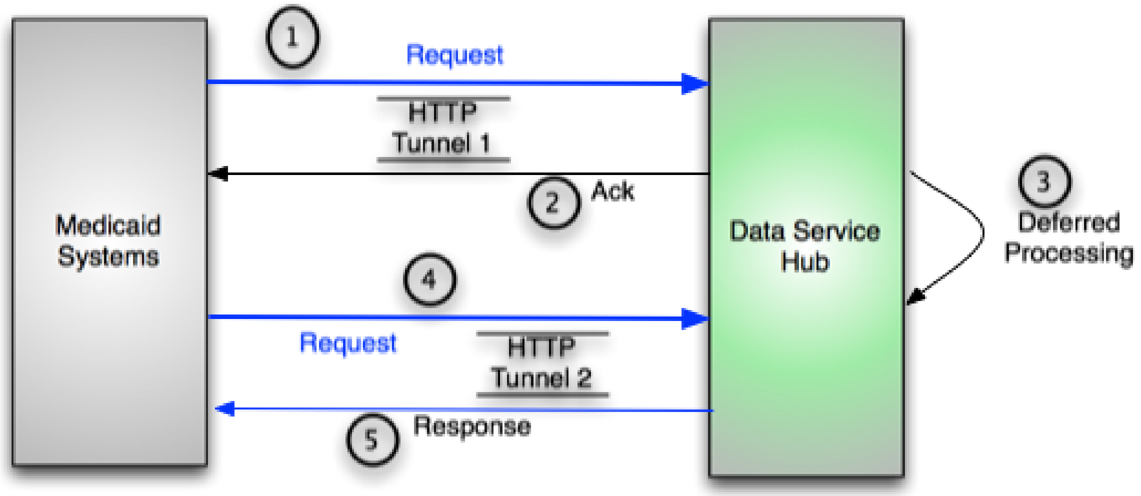
Exception Handling and Other Notes

- At any time, if the connectivity is lost the transaction is not lost as long as it has been received and accepted by the FDSH.

- The FDSH triggers a timeout error if the TDS is not responding to the request within the SLA threshold. The timeout error is communicated as an error message back to the SBE/Medicaid System.

Asynchronous Communication Data Exchange Pattern with Pull Method for Response

The requestor (SBE/Medicaid CHIP E&E System) must either create a new service to process the response (call back mechanism with EPR), or develop an additional service into FDSH infrastructure to check and validate the other business metrics. This is shown as the pull method for response in the following diagram.



Batch Process/Electronic File Transfer

This section will include the defined processes, file types (e.g., XML, FTP, and CSV), time events, messaging, acknowledgements, reporting, etc. for batch processing.

In the context of the FDSH, certain transaction file sets will be created and sent to the FDSH so they can be executed to completion without manual intervention. Input will be preselected and formatted through scripts and/or command-line parameters.

One benefit of FDSH batch processing is moving the time-event of transaction processing within the batch processing framework to when computing resources are less busy as well as providing for high-volume processing.

The characteristics of a typical batch process include:

- A long-running process that must occur on a regularly scheduled basis (re: SLAs).
- There is a high volume of data to be processed.
- For the FDSH, there may be complex logic or calculations to perform for the transaction(s).
- The process is run asynchronously and is not part of a transaction waiting to complete.

Specifications and defined processes for “batch” are currently under discussion with CMS.

Appendix D – TRR Procedures and Checklist

The Test Readiness Review (TRR) will follow a standard set of procedures and use a checklist for each TRR conducted during State testing.

The procedures include:

- Identify all required participants out of the following list of potential stakeholders (assumed that the list includes representatives from CMS as well, if applicable):
    - Testing Point of Contact – CMS and State Leads that have authority to make a Go/No-Go decision for testing to start
    - Testers
    - State Project Team
    - Release Managers from both the State and CMS
    - Security
    - Network Administration
    - System Architects and/or Engineers
    - Operations Support
    - State and CMS project teams that are part of the specific test covered by the TRR
    - System/Release Management and Deployment
    - Meeting recorder
- Timeline
    - CMS and State send out TRR Invitations and Checklist (I&C)
    - CMS and State POCs collect and consolidate I&C responses
    - CMS sends out TRR agenda and Consolidated Checklist
    - TRR meeting – approx. 5 working days prior to Testing Start
- TRR procedure:
    - Invited stakeholders formally walk through the checklist, highlighting missing information, outstanding issues from prior reviews, and "no" answers
    - Based on evidence provided, CMS and the State Leads make a testing go/no-go decision and agree to any adjustments to the plan
    - Testing will only go forward with a unanimous decision by CMS and the State Leads.
    - Annotated TRR checklist becomes the documented minutes for the milestone.

The sample TRR checklist in Table 9 is generic as shown, but will be customized as necessary to document individual State testing needs.

Table 9 - TRR Checklist

Item #	Title	Responsible State Agency (CMS, XXX, others)	Not Used				Criteria Satisfied (Yes / No)	Comments
1	**Previous Test Results / Discrepancy Reports (DRs)**							
	a. Does product documentation describe all known missing or broken functionality in the system as delivered per the Release Plan?							
	b. Are there outstanding problems from previous test phases?							
	c. Are there tests that cannot be fully or partially executed?							
	d. Have the business rules governing open Defect Reports (DR) been met? (e.g., no Severity Level 1 or 2 DRs are allowed to remain open for the upcoming test without a waiver.)							
2	**Test Environment**							The TRR will be tailored to each phase to define what is needed.
	a. Have limitations to the test environment been identified and agreed to?							
	b. Have all required updates been incorporated?							
	c. Is physical connectivity established as required?							
	d. Have all test environments been frozen?							
	e. Have all test environments been scrubbed?							
	f. Are all test environments properly configured, operational, and ready to go?							

Item #	Title	Responsible State Agency (CMS, XXX, others)	Not Used				Criteria Satisfied (Yes / No)	Comments
3	**Test Equipment / Test Tools**							
	a. Are the test equipment and test tools integrated, configured, and ready to use?							
4	**Transmittal Procedures**							
	a. Are transmittal procedures for normal and emergency testing complete and ready to go?							
5	**Security "Checks" Complete (Ready to Test)**							
	a. Has the draft Interconnection Security Agreement been approved?							
	b. Have the security requirements for State testing been met?							
	c. Is the system ready for testing?							
6	**Scenarios / Capabilities**							
	a. Have the scenarios been established and agreed to?							
	b. Have capabilities been established and agreed to?							
7	**Documentation** (e.g., Test Plan, Interface Control Document [ICD], Operator's Manual, Version Description Documents [VDD])							
	a. Is the State Agency Test Plan complete and available?							
	b. Is the ICD complete and available?							
	c. Are the other latest required documents complete and available?							

Item #	Title	Responsible State Agency (CMS, XXX, others)	Not Used				Criteria Satisfied (Yes / No)	Comments
8	**Test Cases**							
	a. Have the required test cases and test procedures been completed?							
	b. Have the required test scripts been completed?							
	c. Have test cases and test scripts been placed under Configuration Management (CM) control?							
9	**Test Data**							
	a. Has the test data been created, loaded, validated, and coordinated/ shared?							
	b. Has the test data been placed under CM control?							
	c. Has the test data been backed up?							
10	**Testers**							
	a. Are all testers identified and confirmed? b. Have contact names and telephone numbers been provided to the test team?							
11	**Stakeholders** (Quality Assurance [QA], Business Owners, Operations, Security, Performance Accessibility, Development)							
	a. Are all required participants/observers identified and engaged?							

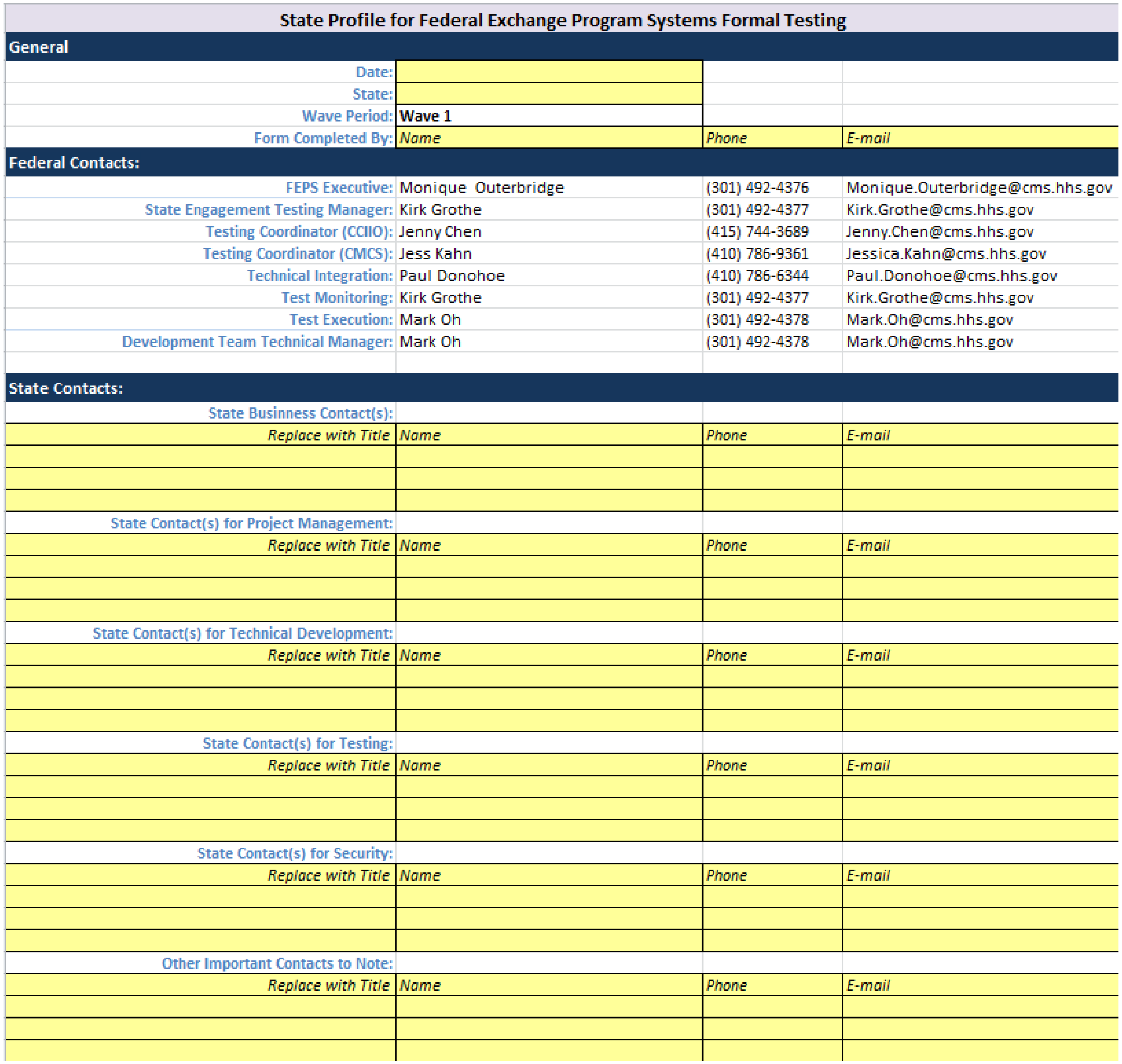
Item #	Title	Responsible State Agency (CMS, XXX, others)	Not Used				Criteria Satisfied (Yes / No)	Comments
12	**State Agency Specialty Testing**							
	a. Has your State completed system/release testing in accordance with the State Agency Test Plan?							
	b. Is performance testing being performed?							
	c. Is accessibility (section 508) testing being performed?							
	d. Are there outstanding issues from the specialty tests?							
13	**Defect Reports (DRs) Tracking / Test Results**							
	a. Is the defect tracking system up, running, and accessible?							
	b. Is an escalation procedure for priority/ severity been established?							
	c. Is there a place to store the test results?							
	d. Have the recipients for test results summaries and/or reports been identified?							
14	**Logistical and “Emergency” Contact Information**							
	a. Are procedures for operational and emergency communications established and documented?							
	b. Are all operational and emergency points of contacts identified and available to the testers?							

Item #	Title	Responsible State Agency (CMS, XXX, others)	Not Used				Criteria Satisfied (Yes / No)	Comments
15	**Testing Schedule / Priorities**							
	a. Is the overall (high-level) testing schedule complete, current, and available?							
	b. Is the detailed phase-specific testing schedule complete, current, and available?							
	c. Does the testing schedule reflect the agreed-upon testing priorities and available resources?							
	d. Has a method for status reporting and frequency been established and agreed to?							
16	**Roles / Responsibilities – "User Accounts"**							
	a. Do the testers have the required Physical Access for the planned testing?							
	b. Do the testers have the required System Access with the appropriate user rights and permission levels for the planned testing?							
17	**<u>Final Disposition</u>**							
	a. Have all Test-Ready Entrance Criteria been met?							
	i) If not, which criteria were not demonstrated?							
	b. Is a follow-up TRR needed?							
	i) If yes, when will the TRR be scheduled?							
	ii) Is the follow-up TRR scheduled?							
	c. Has delivery of a Test Results Summary and/or Report to the required recipients been scheduled?							

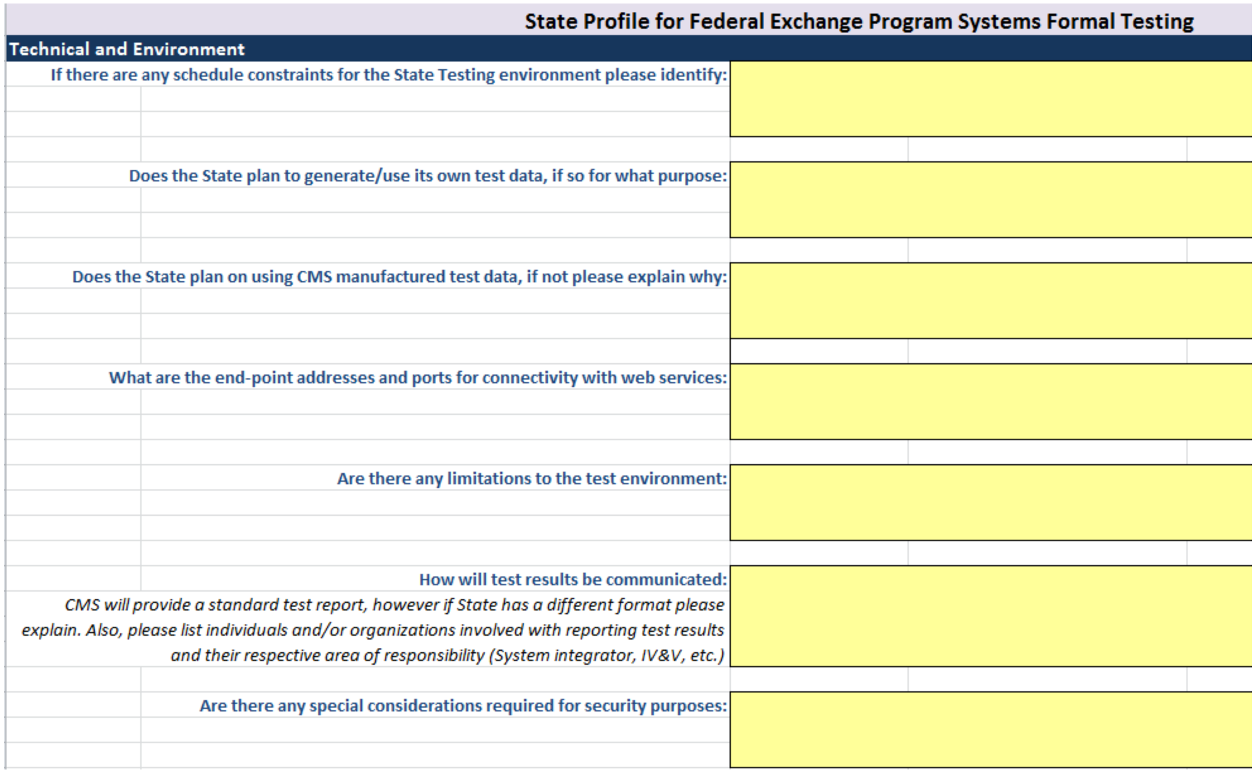
Item #	Title	Responsible State Agency (CMS, XXX, others)	Not Used				Criteria Satisfied (Yes / No)	Comments
	d. Have previous State agency test phases been completed?							

Appendix E – State Testing Profile Template

The Following State Testing Profile is a sample. Each State Testing Profile will be uniquely designed to that State’s Exchange model.



State Profile for Federal Exchange Program Systems Formal Testing			
General			
Date:			
State:			
Wave Period:	Wave 1		
Form Completed By:	*Name*	*Phone*	*E-mail*
Federal Contacts:			
FEPS Executive:	Monique Outerbridge	(301) 492-4376	Monique.Outerbridge@cms.hhs.gov
State Engagement Testing Manager:	Kirk Grothe	(301) 492-4377	Kirk.Grothe@cms.hhs.gov
Testing Coordinator (CCIIO):	Jenny Chen	(415) 744-3689	Jenny.Chen@cms.hhs.gov
Testing Coordinator (CMCS):	Jess Kahn	(410) 786-9361	Jessica.Kahn@cms.hhs.gov
Technical Integration:	Paul Donohoe	(410) 786-6344	Paul.Donohoe@cms.hhs.gov
Test Monitoring:	Kirk Grothe	(301) 492-4377	Kirk.Grothe@cms.hhs.gov
Test Execution:	Mark Oh	(301) 492-4378	Mark.Oh@cms.hhs.gov
Development Team Technical Manager:	Mark Oh	(301) 492-4378	Mark.Oh@cms.hhs.gov
State Contacts:			
State Business Contact(s):			
Replace with Title	*Name*	*Phone*	*E-mail*
State Contact(s) for Project Management:			
Replace with Title	*Name*	*Phone*	*E-mail*
State Contact(s) for Technical Development:			
Replace with Title	*Name*	*Phone*	*E-mail*
State Contact(s) for Testing:			
Replace with Title	*Name*	*Phone*	*E-mail*
State Contact(s) for Security:			
Replace with Title	*Name*	*Phone*	*E-mail*
Other Important Contacts to Note:			
Replace with Title	*Name*	*Phone*	*E-mail*



State Profile for Federal Exchange Program Systems Formal Testing

Technical and Environment

If there are any schedule constraints for the State Testing environment please identify:

Does the State plan to generate/use its own test data, if so for what purpose:

Does the State plan on using CMS manufactured test data, if not please explain why:

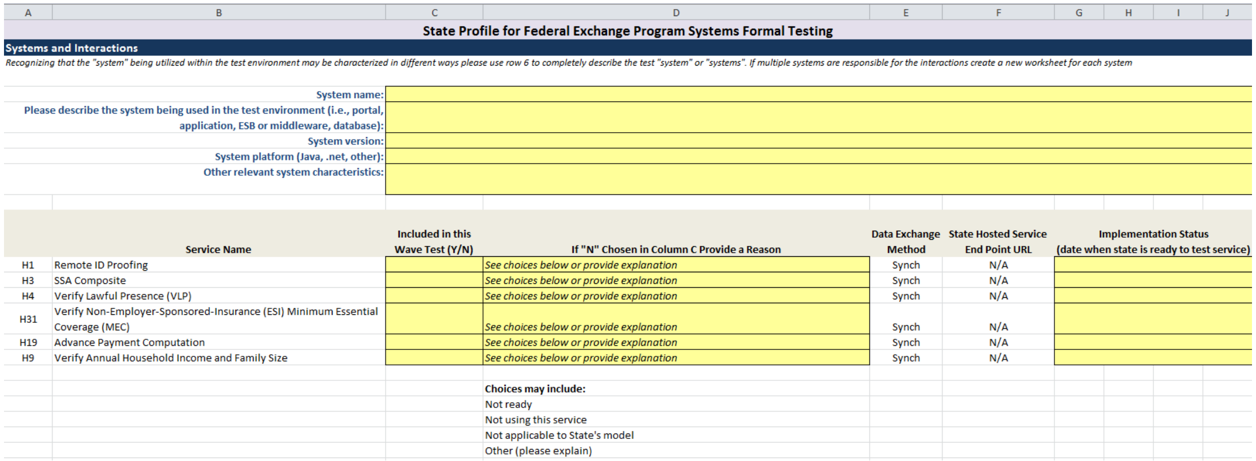
What are the end-point addresses and ports for connectivity with web services:

Are there any limitations to the test environment:

How will test results be communicated:

CMS will provide a standard test report, however if State has a different format please explain. Also, please list individuals and/or organizations involved with reporting test results and their respective area of responsibility (System integrator, IV&V, etc.)

Are there any special considerations required for security purposes:



State Profile for Federal Exchange Program Systems Formal Testing

Systems and Interactions

Recognizing that the "system" being utilized within the test environment may be characterized in different ways please use row 6 to completely describe the test "system" or "systems". If multiple systems are responsible for the interactions create a new worksheet for each system

System name:

Please describe the system being used in the test environment (i.e., portal, application, ESB or middleware, database):

System version:

System platform (Java, .net, other):

Other relevant system characteristics:

	Service Name	Included in this Wave Test (Y/N)	If "N" Chosen in Column C Provide a Reason	Data Exchange Method	State Hosted Service End Point URL	Implementation Status (date when state is ready to test service)
H1	Remote ID Proofing		*See choices below or provide explanation*	Synch	N/A	
H3	SSA Composite		*See choices below or provide explanation*	Synch	N/A	
H4	Verify Lawful Presence (VLP)		*See choices below or provide explanation*	Synch	N/A	
H31	Verify Non-Employer-Sponsored-Insurance (ESI) Minimum Essential Coverage (MEC)		*See choices below or provide explanation*	Synch	N/A	
H19	Advance Payment Computation		*See choices below or provide explanation*	Synch	N/A	
H9	Verify Annual Household Income and Family Size		*See choices below or provide explanation*	Synch	N/A	

Choices may include:
Not ready
Not using this service
Not applicable to State's model
Other (please explain)